

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ «API Gateway»

1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГИ

- 1.1. Услуга предоставляет возможность создания, публикации, конфигурирования, мониторинга и использования высокопроизводительных, полностью управляемых API-шлюзов. API-шлюзы позволяют выполнять множество задач: принимать, обрабатывать и распределять запросы, контролировать трафик, осуществлять быстрое масштабирование, выполнять интеграцию с облачными сервисами, осуществлять контроль доступа и настройку безопасности, выполнять мониторинг API.
- 1.2. В рамках Услуги Исполнитель предоставляет Заказчику возможность:
- создания, настройки и конфигурирования, а также управления жизненным циклом API-шлюзов;
 - создания, настройки и конфигурирования, а также управления жизненным циклом правил, задающих логику обработки входящих запросов к API-шлюзам;
 - использования данных правил для организации маршрутизации запросов к API по заданному сценарию.

- 1.3. Управление API шлюзами осуществляется при помощи консоли управления API Gateway в составе Платформы.

- 1.4. Состав и основные компоненты Услуги:

Табл.1. Состав и основные компоненты

Ресурсы	
Наименование группы	Содержание
API Gateway	<ul style="list-style-type: none">- Конфигурация API-шлюза;- Правила API-шлюза;- Модули, расширяющие функциональность правил API-шлюза (плагины).

Услуга представляет собой набор компонентов для управления API-шлюзами:

- Конфигурация API-шлюза предоставляет возможность создания шлюза API для дальнейшей отправки запросов на URL шлюза и обработки таких запросов Правилами API-шлюза. Шлюз поддерживает работу через HTTPS и через Websockets.
 - Правила API-шлюза предоставляют основные функциональные возможности внутри API-шлюза и используются для обработки запросов, поступивших на описанные URI API-шлюза:
 - Маршрутизация запросов в целевые сервисы Пользователя;
 - Разделение трафика для распределения запросов между двумя и более сервисами Пользователя;
 - Создание API-заглушек для получения ответа от шлюза API, минуя подключение к клиентскому сервису;
 - Может быть реализована иная функциональность, направленная на обработку входящих запросов.
 - Модули, расширяющие функциональность правил API-шлюза (плагины), дополняют настройки правил для реализации сложных бизнес-сценариев и предоставляют следующие возможности:
 - Ограничение количества запросов в единицу времени;
 - Перезапись ответа от сервиса пользователя;
 - Возможность кэширования ответов;
 - Настройка авторизации;
 - Совместное использование ресурса (CORS),
 - Может быть реализована иная функциональность, направленная на обработку входящих запросов.
- 1.5. В целях обеспечения защиты Инфраструктуры используются следующие уровни защиты:

Табл.2. Обеспечение защиты Инфраструктуры

Уровни защиты	Мероприятия
Защита Облака Cloud и средств его управления	
Физический	Обеспечивается: – размещение всего оборудования Инфраструктуры в ЦОД, соответствующих требованиям надежности по категории Tier 3; – контроль и управление доступом к оборудованию; – наличие системы видеонаблюдения на объектах информатизации ЦОД.
Сетевой	Обеспечивается защита периметра Инфраструктуры с использованием межсетевых экранов нового поколения (NGFW), осуществляющих в том числе выявление и предотвращение компьютерных атак.
Инфраструктурный	Обеспечивается: – двухфакторная аутентификация администраторов Инфраструктуры; – подключение администраторов Инфраструктуры к средствам ее управления с использованием VPN; – контроль действий привилегированных пользователей (администраторов Инфраструктуры) с использованием специализированных средств; – регулярный контроль и анализ защищенности Инфраструктуры с использованием специализированных средств по выявлению уязвимостей в используемом ПО и его некорректной конфигурации, влияющей на уровень защищенности ПО, с устранением выявленных уязвимостей и/или недостатков; – сбор и анализ событий информационной безопасности.
Дополнительный	Осуществляются периодические тестирования на проникновение и аудит информационной безопасности Облака Cloud с привлечением сторонних организаций. Выявленные в ходе соответствующего тестирования и/или аудита недостатки устраняются по факту их выявления.
Изоляция Заказчиков	
Межсетевое экранирование	Используются средства межсетевого экранирования для обеспечения контроля и фильтрации информационных потоков, проходящих к веб-серверу и от веб-сервера.
Шифрование трафика	Пользовательский трафик передаётся в зашифрованном виде (HTTPS) и шифруется при помощи подписанного и надежного сертификата.
Управление доступом	Осуществляется управление учетными записями. Устанавливается ограничение на количество неуспешных попыток входа в систему. Производится регистрация событий безопасности.

- 1.6. Распределение ролей, обязанностей и ответственности в области ИБ в отношении Услуги описано в Таблице № 3.

Табл. 3. Распределение ролей, обязанностей и ответственности в области ИБ

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/ сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
Прикладной уровень и уровень использования услуги Заказчиком	Журналирование событий	Журналирование событий доступа к целевым хостам, на которые выполняется перенаправление запросов	Заказчик	Заказчик
	Управление доступом	Настройка доступов к использованию Правил API-шлюза, или использование правил с публичным доступом	Заказчик	Заказчик
	Управление аутентификационной информацией	Управление аутентификационной информацией, используемой для доступа к эндпоинтам, создаваемыми Правилами API-шлюза	Заказчик	Заказчик
	Обеспечение защиты персональных данных клиентов	Защита согласно 152-ФЗ персональных данных (ПДн) клиентов, обрабатываемых в рамках использования API-шлюзов	Заказчик и Исполнитель	Заказчик
Уровень «Организации»	Журналирование событий	Журналирование событий, связанных с функционированием шлюза API: 1. Создание и удаление шлюза API, 2. Создание, публикация, изменение, удаление правила, 3. Создание, изменение, удаление подключения к сервису пользователя, 4. Создание, изменение, удаление авторизационных данных для использования в рамках Правил.	Исполнитель	Заказчик
	Управление аутентификационной информацией	Создание/удаление новых учётных записей в составе организации заказчика	Исполнитель	Заказчик
Инфраструктурный уровень	Мониторинг и поддержка	Мониторинг Инфраструктуры API Gateway, обеспечение её доступности, производительности, наличия необходимого количества оборудования, обеспечение необходимой для её работы пропускной способности сети, вычислительных мощностей.	Исполнитель	Исполнитель
	Журналирование событий	Журналирование событий в компонентах и средствах защиты информации Инфраструктуры API Gateway	Исполнитель	Исполнитель
	Управление доступом	Управление доступом к сегменту управления Инфраструктурой API Gateway	Исполнитель	Исполнитель
	Управление конфигурацией	Контроль и управление процессами изменения конфигурации Инфраструктуры API Gateway	Исполнитель	Исполнитель
	Управление безопасностью для виртуальных и физических сетей	Защита периметров ЦОД Инфраструктуры API Gateway с использованием кластеров высокопроизводительных межсетевых экранов нового поколения (NGFW), обеспечивающих межсетевое экранирование и защиту от компьютерных атак Инфраструктуры. Защита сетевой Инфраструктуры API Gateway (входа в облако) от DDoS-атак, направленных на переполнение канальной емкости. Внутреннее сегментирование сетевых Инфраструктур ENT с использованием NGFW и выделением в рамках ЦОД на сетевом уровне DMZ, PROD- и MGMT-сегментов Инфраструктуры	Исполнитель	Исполнитель

Табл. 3. Распределение ролей, обязанностей и ответственности в области ИБ

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/ сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
	Установка и администрирование средств защиты	Установка, настройка и администрирование средств защиты информации в составе Инфраструктуры, в том числе: 1. средств антивирусной защиты; 2. средств контроля действий привилегированных пользователей (администраторов SberCloud) класса PIM&PAM; 3. SIEM; 4. средств контроля и анализа защищенности; 5. WEB Application Firewall (WAF), используемого для защиты публикуемых KY ENT; 6. NGFW; 7. Identity and access management (IAM)	Исполнитель	Исполнитель
	Обеспечение защиты персональных данных клиентов	Защита ПДн сотрудников Заказчика, имеющих доступ к КУ, обрабатываемых в Инфраструктуре исполнителя	Исполнитель	Исполнитель
Физический уровень	Контроль доступа	Контроль доступа в ЦОД и помещения Инфраструктуры API Gateway (охраняемая территория ЦОД, пропускной режим, системы контроля и управления доступом, запирающие стоек)	Исполнитель	Исполнитель
	Видеонаблюдение	Наличие внешней (по периметру ЦОД) и внутренней (в машинных залах ЦОД) систем видеонаблюдения	Исполнитель	Исполнитель
	Размещение оборудования	Предоставление электропитания, доступа к сети Интернет и свободного места в стойках ЦОД. Предоставление, монтаж и коммутация оборудования (compute, network) в стойках ЦОД.	Исполнитель	Исполнитель

- 1.7. Для подключения к Услуге Заказчик может выбрать один или несколько типов подключения:

Табл.4. Типы подключения к сети и сетевые сервисы

Тип подключения	Описание
Подключение через сеть Интернет	Предполагает логическое подключение к общему для всех Заказчиков Услуги каналу передачи данных. Скорость сетевого соединения для каждого Заказчика не является гарантированной и зависит от загруженности общего канала передачи данных (Услуга предоставляется по умолчанию).
Подключение через выделенный канал связи	Способ подключения, позволяющий гарантировать параметры канала связи. Выделенный канал связи состоит из двух частей: <ol style="list-style-type: none"> 1. Канал связи от инфраструктуры Заказчика к узлу связи Cloud, расположенному на ММТС-9, ММТС-10 2. От ММТС-9, ММТС-10 до Инфраструктуры

- 1.8. **Программная платформа.** Услуга реализована на базе микросервисной архитектуры, размещенной в контуре управления Исполнителя, и состоит из следующих сервисов:

- Ядро продукта, отвечающее за функциональную часть работы продукта;
- Слой, реализующий возможность работы с ядром из пользовательского интерфейса;
- Компонент сбора данных мониторинга;
- Компонент, отвечающий за управление жизненным циклом продукта;
- Компонент, отвечающий за сбор тарификационных данных.

- 1.9. **Аппаратная платформа:**

Табл.5. Компоненты и характеристики аппаратной платформы

Компоненты	Характеристики
Технологическая платформа	В качестве технологической вычислительной платформы используется кластер Managed Kubernetes с горизонтальным масштабированием.
Сеть	Базируется на оборудовании ведущих производителей, которое обеспечивает: <ul style="list-style-type: none"> – высокий уровень контроля и безопасности благодаря потоковой телеметрии и упреждающему анализу на линейной скорости передачи; – высокую производительность приложений благодаря интеллектуальным буферам и отсутствию потери пакетов; – высокую производительность и масштабируемость благодаря мультискоростным портам 1/10/25/50/100G. Сетевая подсистема реализована с применением топологии Leaf - Spine, которая обеспечивает следующие преимущества: <ul style="list-style-type: none"> – предсказуемость задержек; – высокий уровень масштабируемости без прерывания работы сети; – защиту от появления петель; – высокий уровень автоматизации управления и поддержки.

- 1.10. **Мониторинг**

Предоставляется возможность просматривать статистику потребления Услуги. Для мониторинга доступны:

- количество запросов за период;
- объем трафика за период;
- время задержки для входящего потока трафика;
- время задержки для исходящего потока трафика.

- 1.11. **Требования к инфраструктуре Заказчика:**

- наличие доступа в Интернет.

- 1.12. **Технические особенности и ограничения:**

- скорость сетевого соединения для каждого Заказчика, в случае подключения через Интернет, не является гарантированной и зависит от утилизации общего интернет-канала в зоне доступности Услуги;
- суммарное время выполнения запросов включает в себя время, затраченное на обработку запроса сервисом пользователя, и может зависеть от производительности инфраструктуры Заказчика;
- при настройке нескольких Правил API-шлюза в рамках одного API-шлюза, входящий запрос может быть обработан несколькими Правилами API-шлюза. В этом случае, в тарификацию будет включено количество запросов, соответствующее количеству правил, обрабатывающих этот запрос;

- Некорректная настройка правил может привести к возникновению коллизии между URI шлюза API, использованных в нескольких Правилах API-шлюза. В этом случае, будет использовано только одно из правил. Контроль за отсутствием коллизий осуществляет Заказчик.

2. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И МЕТРИКИ УСЛУГИ

2.1. Параметры Услуги описаны в Таблице 6:

Табл.6. Параметры предоставляемых Услуг

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Входящие запросы	Вызовы API, количество (шт.)	-	-
Сетевые сервисы	Объем переданного исходящего трафика по сети (КБ)	-	-

3. ТАРИФИКАЦИЯ УСЛУГИ

- 3.1. Тарификация Услуги динамическая (Pay as you Go). Динамическая тарификация предполагает оплату пула ресурсов, указанных ниже, по факту их потребления Заказчиком в течение Отчетного периода.
- 3.2. Величина ежемесячного платежа за пользование Услугой определяется в соответствии с фактическим потреблением перечисленных ниже ресурсов. Доступные ресурсы и опции перечислены в Таблице 7.

Табл.7. Параметры потребления API-шлюзов

Наименование ресурса	Единицы измерения	Кратность подсчета
Количество запросов к API-шлюзам	Шт.	1
Объем переданного исходящего трафика по сети	КБ	1

- 3.3. Методика расчётов потребляемых ресурсов предполагает тарификацию суммы значений предоставленных услуг за Отчетный период в соответствии с Тарифом. Счет выставляется на основе суммы значений за период оказания услуг.

4. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

- 4.1. Возможные виды подключения / изменения / отключения Услуг:
- посредством совершения действий в Личном кабинете.
- 4.2. Возможный порядок расчётов по Услуге:
- постоплата.
- 4.3. Возможные способы оплаты / порядок пополнения баланса:
- оплата в безналичном порядке на основании выставленного Исполнителем счёта.